UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/975,302	10/12/2001	Ari Hypponen	108347-00011	6981

4372 7590 10/06/2004

ARENT FOX KINTNER PLOTKIN & KAHN
1050 CONNECTICUT AVENUE, N.W.
SUITE 400
WASHINGTON, DC 20036

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/975,302	HYPPONEN, ARI
	Examiner	**Art Unit**
	Ronald Baum	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-8 are pending for examination.

2. Claims 1-8 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-8 are rejected under 35 U.S.C. 102(b) as being anticipated by Blakley, III et al, U.S. Patent 5,677,952.

4. As per claim 1; "A method of securing data stored on an electronic device, the method comprising encrypting the data using a cryptographic key derivable from or accessed using a passphrase, requiring the entry into the device of the passphrase when a user wishes to access the data, subsequently inhibiting access to the data whilst the device remains active, and requiring the entry into the device of a predefined password when a user wishes to access the data, the password being different from the passphrase [col. 1,lines 10-col. 11,line 13, whereas the use of a secret key derived from the user entered password information (a password is broadly interpreted by the examiner to be a pass phrase per se since the digital representation of the password consisting of multiple bits would correspond to multiple pieces of information that typically constitutes a pass phrase) is used for the information (i.e., file on a hard drive) encryption security. Further, since to subsequently access the stored encrypted data file, the

access request must be made, for example by specifying a file name or "clicking" on a file icon, such that the specifying function/method will inherently produce an index (i.e., track/sector HDD addressing of the file, which is an index); then the access to said file in the form of the request is a function of the index, which is the same index used to specify the access requirements when the file was stored encrypted. Still further, the access 'to the data whilst the device remains active' is broadly interpreted to encompass the computer powered up with the secret key stored in the computer volatile memory (i.e., col. 3,lines 34-44, col. 6,lines 48-58, col. 10,lines 53-63, specifically, typically PC DRAM memory).].";

Further, as per claim 6; "Apparatus [This claim is the apparatus (system) claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] for securing electronic data, the apparatus comprising: a memory for storing encrypted and unencrypted data: first processing means for encrypting data using a cryptographic key derivable from or accessed using a passphrase; input means for receiving the passphrase from a user when the user wishes to access the data; second processing means for subsequently inhibiting access to the data whilst the device remains active, and for requiring the entry into the device of a predefined password via said input means when a user wishes to access the data, the password being different from the passphrase.";

Further, as per claim 8; "A computer storage medium [This claim is the embodied software claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] having stored thereon a program for causing a computer device to secure data stored on the electronic device by: encrypting the data using a cryptographic key derivable from or accessed using a passphrase, requiring the entry into the device of the passphrase when a user wishes to access the data, subsequently inhibiting access to the data whilst the device remains active, and requiring the entry into the device of a predefined password when a user wishes to access the data, the password being different from the password.".

5. Claim 2 ***additionally recites*** the limitation that; "A method according to claim 1, wherein, following inhibition of data access, the device requires that the user enter the correct password within a predefined number of attempts, and, if the user fails to enter the correct password within this number of attempts, the cryptographic key stored by the device is deleted, and the user requested to reenter the correct passphrase.". The teachings of Blakley, III et al suggest such limitations (i.e., col. 1,lines 10-col. 11,line 13, whereas the use of "ending the computer session… as a function of predetermined timeout period" (i.e., col. 2,lines 23-43, col. 6,lines 47-57, col. 10,lines 50-65), are broadly interpreted to encompass the "predefined number of attempts" limitations whereas the crypto key is deleted.).

6. Claim 3 ***additionally recites*** the limitation that; "A method according to claim 2, wherein, if the correct passphrase is not reentered by the user, the encrypted data may only be accessed by entering the cryptographic key into the device.". The teachings of Blakley, III et al suggest such limitations (i.e., col. 1,lines 10-col. 11,line 13, whereas the use of "ending the computer session… as a function of predetermined timeout period" (i.e., col. 2,lines 23-43, col. 6,lines 47-57, col. 10,lines 50-65), are broadly interpreted to encompass the "encrypted data may only be accessed by entering the cryptographic key into the device" limitations whereas the crypto key having been deleted would inherently be a function of the computer loosing power, etc., such

that key re-entry subsequently would be inherent. Still further, the access "only be accessed by entering the cryptographic key into the device" is broadly interpreted to encompass the computer powered up with the secret key stored in the computer volatile memory (i.e., col. 3,lines 34-44, col. 6,lines 48-58, col. 10,lines 53-63, specifically, typically PC DRAM memory).).

7. Claim 4 ***additionally recites*** the limitation that; "A method according to claim 1 and comprising storing the predefined password in a memory of the device following encryption with said password or said cryptographic key, and verifying the password entered by the user by comparing it with the stored password.". The teachings of Blakley, III et al suggest such limitations (i.e., col. 1,lines 10-col. 11,line 13, whereas the use of a secret key derived from the user entered password information is used for the information (i.e., file on a hard drive) encryption security (and clearly stored in the process). Further, since to subsequently access the stored encrypted data file, the access request must be made, for example by specifying a file name or "clicking" on a file icon, such that the specifying function/method will inherently produce an index (i.e., track/sector HDD addressing of the file, which is an index); then the access to said file in the form of the request is a function of the index, which is the same index used to specify the access requirements when the file was stored encrypted (and clearly stored in the process). Still further, the access "verifying the password entered by the user by comparing it with the stored password" is broadly interpreted to encompass the computer powered up with the secret key stored in the computer volatile memory (i.e., col. 3,lines 34-44, col. 6,lines 48-58, col. 10,lines 53-63, specifically, typically PC DRAM memory).).

8. Claim 7 ***additionally recites*** the limitation that; "Apparatus according to claim 6, the apparatus being a mobile computer device such as a laptop or palmtop computer, a PDA, or a mobile telephone.". The teachings of Blakley, III et al suggest such limitations (i.e., col. 1,lines 42-62, col. 3,lines 19-33).

9. As per claim 5; "A method of preventing unauthorized access to electronic data stored on a computer device, the method comprising: requesting a user to input a passphrase into the device; receiving an entered passphrase and using the passphrase to generate or access a cryptographic key; storing the cryptographic key in a memory of the device, wherein the stored key can be used to subsequently encrypt and decrypt data on the device; subsequently inhibiting a user from accessing data on the device after a predefined period, or after a predefined period of non-use, or after some predefined action by the user; requesting a user to input a password into the device; receiving the password and, only if the password corresponds to a predefined password which is different from said passphrase, allowing the user to access data on the device, otherwise continuing to inhibit a user from accessing data on the device [This claim is the combination of claims 1,2 above, and is rejected for the same reasons provided for the claims 1,2 rejection].".

Conclusion

10. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum
Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100